

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-57112

(P2000-57112A)

(43) 公開日 平成12年2月25日 (2000.2.25)

(51) Int.Cl. ⁷	識別記号	F I	ターマコード* (参考)
G 0 6 F 15/16	6 2 0	G 0 6 F 15/16	6 2 0 B 5 B 0 4 5
13/00	3 5 1	13/00	3 5 1 Z 5 B 0 8 9
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 A 5 J 1 0 4
	6 6 0		6 6 0 E
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A
審査請求 未請求 請求項の数22 O L (全 18 頁)			

(21) 出願番号 特願平10-226430

(22) 出願日 平成10年8月11日 (1998.8.11)

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 堀切 和典

神奈川県足柄上郡中井町境430グリーンテ

クなかい 富士ゼロックス株式会社

(74) 代理人 100086531

弁理士 澤田 俊夫

Fターム(参考) 5B045 G06 JJ33 JJ35 KK03

5B089 GA11 GA19 GB09 KA17 KC47

KC53 KC58 KH30

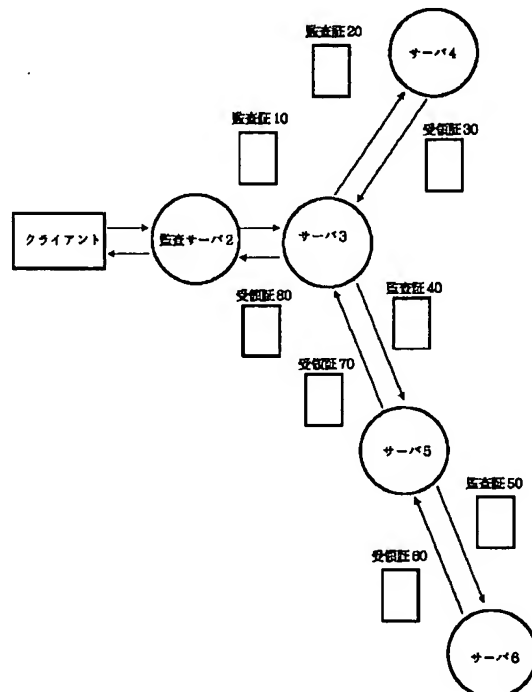
5J104 AA07 KA01 PA07

(54) 【発明の名称】 ネットワーク上で遠隔手続き呼び出しを実行するための方法、及び、遠隔手続き呼び出しを実行可能なネットワーク・システム

(57) 【要約】

【課題】 サービス要求の出所を認証したり、サーバから提供されたサービスを保証することができる遠隔手続き呼び出し方式を提供する。

【解決手段】 中継サーバは、クライアントからの要求メッセージを受信すると、これに署名を付けてサーバに送信する。サーバは、中継サーバを認証してサービス要求の出所を確認するとともに、応答メッセージには署名を付けて、中継サーバに応答メッセージを送信する。中継サーバは、署名を認証して、さらに、応答メッセージが正当かどうか検査してから、要求元クライアントに送信する。また、中継サーバは、メッセージの送受信の履歴を記録し、ネットワーク上の不信任動作を監視する。



【特許請求の範囲】

【請求項 1】 サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、 (a) 中継・監査サーバが、クライアントからの第 1 の要求メッセージを受信するステップと、 (b) 前記中継・監査サーバが、第 1 の要求メッセージの要求先である第 1 のサーバに対して第 2 の要求メッセージを送信するステップと、 (c) 前記第 1 のサーバが、受信した第 2 の要求メッセージを受信するとともに、第 2 の要求メッセージが前記中継・監査サーバを経由したことを検査するステップと、 (d) 前記第 1 のサーバが、第 2 の要求メッセージに回答した第 1 の応答メッセージを前記中継・監査サーバに送信するステップと、 (e) 前記中継・監査サーバが、受信した第 1 の応答メッセージが正当なメッセージであることを検査するステップと、 (f) 前記中継・監査サーバが、第 2 の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 2】 前記第 1 のサーバは、さらに、前記第 2 の要求メッセージの少なくとも一部の処理を委ねた第 3 の要求メッセージを第 2 のサーバに送信するとともに、前記第 2 のサーバから受信した応答メッセージとともに前記第 1 の応答メッセージを前記中継・監査サーバに送信する、ことを特徴とする請求項 1 に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 3】 前記ステップ (c) における検査が異常であれば、前記第 1 のサーバは受信した第 2 の要求メッセージの処理を実行しないことを特徴とする請求項 1 又は 2 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 4】 前記ステップ (e) における検査が異常であれば、前記中継・監査サーバは第 2 の応答メッセージを前記クライアントに送信しないことを特徴とする請求項 1 又は 2 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 5】 さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含むことを特徴とする請求項 1 又は 2 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 6】 サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、 (a) 中継・監査サーバが、クライアントからの第 1 の要求メッセージを受信するとともに、ユーザを特定するステップと、 (b) 前記中継・監査サーバが、第 1 の要求メッセージの要求先である第 1 のサーバに対して第 2 の要求メッセージを送

信するステップと、 (c) 前記第 1 のサーバが、受信した第 2 の要求メッセージを受信するとともに、前記中継・監査サーバからのメッセージであることを特定するステップと、 (d) 前記第 1 のサーバが、第 2 の要求メッセージに回答した第 1 の応答メッセージを前記中継・監査サーバに送信するステップと、 (e) 前記中継・監査サーバが、受信した第 1 の応答メッセージが正当なメッセージであることを検査するステップと、 (f) 前記中継・監査サーバが、第 2 の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 7】 前記第 1 のサーバは、さらに、前記第 2 の要求メッセージの少なくとも一部の処理を委ねた第 3 の要求メッセージを第 2 のサーバに送信するとともに、前記第 2 のサーバから受信した応答メッセージとともに第 1 の応答メッセージを前記中継・監査サーバに送信する、ことを特徴とする請求項 6 に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 8】 前記ステップ (e) における検査が異常であれば、前記中継・監査サーバは第 2 の応答メッセージを前記クライアントに送信しないことを特徴とする請求項 6 又は 7 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 9】 さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含むことを特徴とする請求項 6 又は 7 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 10】 サービスを要求する 1 以上のクライアントとサービス・オブジェクトを有する 1 以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、 (a) 中継・監査サーバが、クライアントからの第 1 の要求メッセージを受信するステップと、 (b) 前記中継・監査サーバが、第 1 の要求メッセージの要求先である第 1 のサーバに対して、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けた第 2 の要求メッセージを送信するステップと、

(c) 前記第 1 のサーバが、受信した第 2 の要求メッセージを受信するとともに、前記中継・監査サーバの公開鍵を用いて認証するステップと、 (d) 前記第 1 のサーバが、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、第 2 の要求メッセージに回答した第 1 の応答メッセージを前記中継・監査サーバに送信するステップと、 (e) 前記中継・監査サーバが、第 1 の応答メッセージを受信し、前記第 1 のサーバの公開鍵を用いて認証するとともに、正当なメッセージであることを検査するステップと、 (f) 前記中継・監査サーバが、第 2 の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔

3

手続き呼び出しを実行するための方法。

【請求項 11】前記第 1 のサーバは、さらに、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、前記第 2 の要求メッセージの少なくとも一部の処理を委ねた第 3 の要求メッセージを第 2 のサーバに送信し、前記第 2 のサーバは、前記第 2 のメッセージを受信して、前記第 1 のサーバの公開鍵を用いて認証するとともに、これに回答した応答メッセージを自身の公開鍵暗号系の秘密鍵を用いた署名を付けて前記第 1 のサーバに送信し、

前記第 1 のサーバは、受信した応答メッセージを前記第 2 のサーバの公開鍵を用いて認証した後に、第 1 の応答メッセージを前記中継・監査サーバに送信する、ことを特徴とする請求項 10 に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 12】前記ステップ (c) における認証が異常であれば、前記第 1 のサーバは受信した第 2 の要求メッセージの処理を実行しないことを特徴とする請求項 10 又は 11 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 13】前記ステップ (e) における認証が異常であれば、前記中継・監査サーバは第 2 の応答メッセージを前記クライアントに送信しないことを特徴とする請求項 10 又は 11 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 14】さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含むことを特徴とする請求項 10 又は 11 のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項 15】遠隔手続き呼び出しが実行可能なネットワーク・システムであって、

サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、1 以上の中継・監査サーバと、サービス要求メッセージを受信して、正当な経路を介して受信したメッセージであることを検査するとともに、要求されたメッセージに回答した応答メッセージを送信する、サービス・オブジェクトを有する 1 以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項 16】遠隔手続き呼び出しが実行可能なネットワーク・システムであって、

サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信し、その要求元を特定してから要求先のサーバに向けて転送するとともに、受信

4

したサービス応答メッセージを要求元のクライアントに向けて転送する、1 以上の中継・監査サーバと、サービス要求メッセージを受信して、メッセージの送信元を特定するとともに、要求されたメッセージに回答した応答メッセージを送信する、サービス・オブジェクトを有する 1 以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項 17】遠隔手続き呼び出しが実行可能なネットワーク・システムであって、

サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、サービス要求に対する応答メッセージを受信して、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、1 以上の中継・監査サーバと、

サービス要求メッセージを受信して、要求されたメッセージに回答した応答メッセージを送信する、サービス・オブジェクトを有する 1 以上のサーバとを具備し、

前記中継・監査サーバ及びサーバは、メッセージ送信時には自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付け、メッセージ受信時には送信元の公開鍵を用いて認証を行うことを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項 18】前記中継・監査サーバは、受信したサービス応答メッセージが正当なメッセージであることを検査してからサービスの要求元に向けて送信するとともに、要求メッセージ及び／又は応答メッセージの送受信の履歴を記録することを特徴とする請求項 15 乃至 17 のいずれかに記載の遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項 19】サービスを要求する 1 以上のクライアントと要求されたサービスを提供する 1 以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、

サービス要求メッセージを受信する手段と、自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、

サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、を具備することを特徴とするサーバ。

【請求項 20】サービスを要求する 1 以上のクライアントと要求されたサービスを提供する 1 以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、

サービス要求メッセージを受信するとともにその要求元

を特定する手段と、
自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、
サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、
を具備することを特徴とするサーバ。を特徴とするサーバ。

【請求項21】さらに、
受信したサービス応答メッセージが正当なメッセージであることを検査する手段と、
要求メッセージ及び／又は応答メッセージの送受信の履歴を記録する手段と、を含むことを特徴とする請求項19又は20のいずれかに記載のサーバ。

【請求項22】サービスを要求する1以上のクライアントと要求されたサービスを提供する1以上のサーバとで構成されるネットワーク上において実行される遠隔手続き呼び出し動作をサポートする中継・監視サーバであって、
要求メッセージや応答メッセージの送受信を行う送受信部と、
受信した要求メッセージを解析して要求パラメータを抽出する要求メッセージ解析部と、
要求パラメータに所定の情報を連結して電子署名する監査証生成部と、
応答メッセージを解析して、送信元のサーバが電子署名した受領証を抽出する応答メッセージ解析部と、
受領証を電子認証する受領証処理部と、を含むことを特徴とする中継・監視サーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、1以上のサーバと1以上のクライアントからなる分散環境のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための遠隔手続き／メソッド呼び出し方式に係り、特に、少なくとも1つの中継・監査サーバを中継してサービスの要求がサーバに届くようなタイプの遠隔手続き呼び出し／メソッド方式に関する。

【0002】更に詳しくは、本発明は、クライアントが要求するサービスを複数のサーバの協働的な動作によって提供するような分散型のネットワーク環境において、遠隔的に要求されたサービスの履行を保証するための方式に係り、特に、ネットワーク上に中継・監査サーバを介在させることで、サービス要求の出所を認証したり、サーバから提供されたサービスの品質等を保証することができる遠隔手続き呼び出し／メソッド方式に関する。

【0003】

【従来の技術】昨今の情報処理・情報通信の分野における発展は目覚ましいものがある。この種の技術分野においては、コンピュータ・システム同士を相互接続するため

の研究・開発が、従来より活発になされてきた。システム同士を相互接続する主な目的は、複数ユーザによるコンピュータ資源の共有や、情報の共有・流通などである。

【0004】システム間を接続するための伝送媒体すなわち「ネットワーク」としては、大学や事業所の構内など限られた空間内に敷設されたLAN (Local Area Network) の他、LANを専用回線で接続したWAN (Wide Area Network) や、一般公衆回線 (PSTN)、ISDN (Integrated Service Digital Network)、インターネットなど様々である。

【0005】LANは、一般に、ネットワーク上の特定のコンピュータをサーバ (ファイル・サーバ、プリント・サーバ) とし、これを他のクライアントが利用し合うというクライアント・サーバ型として構築される。かかるクライアント・サーバ・モデルでは、プログラムの一部の手続きの実行をネットワーク上の別のコンピュータに委託するというメカニズム、すなわち「遠隔手続き呼び出し (RPC: Remote Procedure Call)」、若しくは「遠隔メソッド呼び出し (RMI: Remote Method Invocation)」が用いられる。遠隔手続きの実行結果は、戻り値として、呼び出した側のコンピュータに返される。また、手許のコンピュータのキーボードやファイルを使ってプログラムへの入力を果たしたり、同じコンピュータのディスプレイやファイルに出力することもできる。

【0006】遠隔手続き若しくは遠隔メソッド呼び出しの仕組みは、LANの世界に限定されず、さらに、インターネットのような広域的なネットワーク上でも利用可能である。インターネット上で利用可能な各種プロトコル、例えば、HTTP (Hyper Text Transfer Protocol)、HTTPS、S-HTTP (secure HTTP)、FTP (File Transfer Protocol)、CORBA (Common ORB Architecture)、IIOP (Internet Inter-ORB Protocol)、JavaRMI (Remote Method Invocation) なども、遠隔手続き／遠隔メソッド呼び出しとして実現される。インターネットの代表的なクライアント・サーバ・モデルは、WWW (World Wide Web) サーバとWWWブラウザとで構成される (周知)。

【0007】WWWサーバは、通常、多数のサービス・オブジェクトを蓄積しており、WWWクライアントからのサービス要求に回答して、インターネット経由でサービスを提供している。サービス・オブジェクトの一例は、WWWクライアント (ブラウザ) のディスプレイ上においてホームページを形成するためのHTML (Hyper Text Markup Language)

ファイルである。WWWサーバが持つ各サービス・オブジェクトの所在は、URL (Uniform Resource Locator) という形式で表される。URLは、インターネット上の各種情報リソースにアクセスする手段 (すなわち通信プロトコル) とリソースの名前を指定する形式、すなわち「プロトコル名: //サーバ名 (/ディレクトリ名...) /ファイル名」という形式で記述される。

【0008】WWWクライアントとしてのブラウザは、WWWサーバに対して、URLに基づいた形式のサービス要求メッセージを送信する。他方、WWWサーバは、サービス要求メッセージを解釈して、要求されたサービスを提供する。但し、サーバは、要求されたサービスをサーバ単体で実行するとは限らず、さらに別のサーバにサービスの一部の提供を委ねることもある。サーバが他のサーバにサービスの提供を要求する方式の1つはCGI (Common Gateway Interface) である (CGIは、それ自体が標準規約となっているため、この規約を遵守しさえすれば、Visual Basic, C, Delphi, Perlなど各種言語でCGIプログラムを作成することができる)。

【0009】例えば、WWWクライアントがブラウザ画面上で検索項目を入力したときは、WWWサーバは、検索の実行と検索結果の送信を他のデータベース・サーバに要求することがある。この場合、データベース・サーバは、CGIなどの仕組みによってWWWサーバに連動して、要求されたサービスの一部を提供する。データベース・サーバは、検索結果を示すテーブル中の該当するカラムの内容を生成し、WWWサーバはテーブルの残りの部分を生成する (図6参照のこと)。

【0010】クライアントからのサービス要求を第1に受け取ったサーバ (仮に「親サーバ」とする) は、ホームページ内の一部のコンテンツの生成を別のサーバ (仮に「子サーバ」とする) に委ねる。そして、親サーバは、自身が生成したコンテンツと子サーバから戻されたコンテンツとからホームページを生成して、クライアントに戻すという訳である。さらに子サーバは自分の子サーバ (「孫サーバ」) にサービスの一部の提供を委ねることもある。

【0011】サービスを提供する複数のサーバの親子関係は、一種の木構造を形成する。図7にはこれを模式的に示している。同図において、サーバBは、クライアントからのサービス要求 (URL) を最初に受け取る親サーバであり、サーバAとCはサーバBの子サーバである。さらに、サーバCから一部のサービスの提供を要求されるサーバDは、サーバBの孫サーバである。

【0012】従来、殆どの場合において、クライアントから要求されたサービスを実行するサーバ、すなわち木構造を構成する各サーバは、全て単一若しくは同系統の団体に所属し、互いの利益は略一致していた (例えば図

6では、データベース・サーバは、WWWサーバと同じ「組織1」に属している)。クライアントが要求したサービスは物理的には複数のサーバの協働的な動作によって提供されるが、クライアントの立場からすれば、このような木構造の仕組みを意識する必要がなく、実質上1つのサーバが責任を持ってサービスを提供すると思うことができた。言い換えれば、クライアントは、サービスの要求先のサーバを信頼するだけで充分だった訳である。

10 【0013】ところが、コンピュータ・ネットワーキングの世界がさらに進化を遂げるに従い、ネットワークを構成する各マシン間の関係も高度に複雑化してくる。例えば、ある特定のサービスを提供するためのサーバの木構造は、別個の団体に跨ったサーバの集合で構成されることもあり得る。例えば図7では、サーバBとデータベース・サーバは「組織1」に所属するが、子サーバAは「組織2」に、子サーバCと孫サーバDは「組織3」に所属している。親サーバBと子サーバCとが、異なる団体に所属して両者の利害が完全には一致しない、ということも予想される。

20 【0014】あるクライアントが有料でサーバBへのアカウントを取得したような場合、クライアントは、サーバBを全面的に信用するであろうし、サーバBも受け取ったアカウント料金に見合ったサービスを提供するよう努め、また、信用を裏切ることを取ってしないであろう。しかしながら、別団体のサーバCは、クライアントに対して何の義務も義理も感じることはなく、或いはクライアントに対し悪意を抱き、正当なサービスの提供を拒否し或いは不当なサービスを行うという可能性もある。

30 【0015】また、子サーバCが親サーバBとは異なる団体に所属するような場合、サーバBがサーバCに対してサービス提供の対価を支払うような、一種の契約関係が成立していることもある。この対価の額が従量制、すなわちクライアントからのサービス要求の回数に応じて定まることもある。このような場合、サーバCは、サーバBに対するダミーのサービス要求を頻繁に発行せしめることによって、対価額すなわち利益を貪ることもできる (図8を参照のこと)。ダミーのサービス要求は、一般ユーザを装った不正クライアントによって容易に発行される。現状のネットワーク環境において、サーバBが、サーバCやダミー・クライアントのような不正行為を取り締まるようなメカニズムはない。

【0016】

50 【発明が解決しようとする課題】本発明の目的は、1以上のサーバと1以上のクライアントからなる分散型のネ

ットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための、優れた遠隔手続き呼び出しを行う方式を提供することにある。

【0017】本発明の更なる目的は、少なくとも1つの中継・監査サーバを中継してサービスの要求がサーバに届くようなタイプの、優れた遠隔手続き呼び出し方式を提供することにある。

【0018】本発明の更なる目的は、クライアントから要求されたサービスを複数のサーバの協働的な動作によって提供するような分散型のネットワーク環境において、サービスの正当な履行を保証するための優れた方式を提供することにある。

【0019】本発明の更なる目的は、ネットワーク上に中継・監査サーバを配設することで、サービス要求の出所を認証したり、サーバから提供されたサービスの品質等を保証することができる、優れた遠隔手続き呼び出し方式を提供することにある。

【0020】

【課題を解決するための手段】本発明は、上記課題を参酌してなされたものであり、その第1の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、(a)中継・監査サーバが、クライアントからの第1の要求メッセージを受信するステップと、

(b)前記中継・監査サーバが、第1の要求メッセージの要求先である第1のサーバに対して第2の要求メッセージを送信するステップと、(c)前記第1のサーバが、受信した第2の要求メッセージを受信するとともに、第2の要求メッセージが前記中継・監査サーバを経由したことを検査するステップと、(d)前記第1のサーバが、第2の要求メッセージに回答した第1の応答メッセージを前記中継・監査サーバに送信するステップと、(e)前記中継・監査サーバが、受信した第1の応答メッセージが正当なメッセージであることを検査するステップと、(f)前記中継・監査サーバが、第2の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【0021】ここで、前記第1のサーバは、さらに、前記第2の要求メッセージの少なくとも一部の処理を委ねた第3の要求メッセージを第2のサーバに送信するとともに、前記第2のサーバから受信した応答メッセージとともに第1の応答メッセージを前記中継・監査サーバに送信するようにしてもよい。

【0022】また、前記ステップ(c)における検査が異常であれば、前記第1のサーバは受信した第2の要求メッセージの処理を実行しないようにしてもよい。

【0023】また、前記ステップ(e)における検査が異常であれば、前記中継・監査サーバは第2の応答メッ

セージを前記クライアントに送信しないようにしてもよい。

【0024】また、さらに、前記中継・監査サーバが要求メッセージ及び/又は応答メッセージの送受信の履歴を記録するステップを含んでいてもよい。

【0025】また、本発明の第2の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、(a)中継・監査サーバが、クライアントからの第1の要求メッセージを受信するとともに、ユーザを特定するステップと、(b)前記中継・監査サーバが、第1の要求メッセージの要求先である第1のサーバに対して第2の要求メッセージを送信するステップと、

(c)前記第1のサーバが、受信した第2の要求メッセージを受信するとともに、前記中継・監査サーバからのメッセージであるしたことを特定するステップと、

(d)前記第1のサーバが、第2の要求メッセージに回答した第1の応答メッセージを前記中継・監査サーバに送信するステップと、(e)前記中継・監査サーバが、受信した第1の応答メッセージが正当なメッセージであることを検査するステップと、(f)前記中継・監査サーバが、第2の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【0026】ここで、前記第1のサーバは、さらに、前記第2の要求メッセージの少なくとも一部の処理を委ねた第3の要求メッセージを第2のサーバに送信するとともに、前記第2のサーバから受信した応答メッセージとともに第1の応答メッセージを前記中継・監査サーバに送信するようにしてもよい。

【0027】また、前記ステップ(e)における検査が異常であれば、前記中継・監査サーバは第2の応答メッセージを前記クライアントに送信しないようにしてもよい。

【0028】また、さらに、前記中継・監査サーバが要求メッセージ及び/又は応答メッセージの送受信の履歴を記録するステップを含んでもよい。

【0029】また、本発明の第3の側面は、サービスを要求する1以上のクライアントとサービス・オブジェクトを有する1以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、(a)中継・監査サーバが、クライアントからの第1の要求メッセージを受信するステップと、(b)前記中継・監査サーバが、第1の要求メッセージの要求先である第1のサーバに対して、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けた第2の要求メッセージを送信するステップと、(c)前記第1のサーバが、受信した第2の要求メッセージを受信するとともに、前記

10

20

30

40

50

中継・監査サーバの公開鍵を用いて認証するステップと、(d)前記第1のサーバが、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、第2の要求メッセージに回答した第1の応答メッセージを前記中継・監査サーバに送信するステップと、(e)前記中継・監査サーバが、第1の応答メッセージを受信し、前記第1のサーバの公開鍵を用いて認証するとともに、正当なメッセージであることを検査するステップと、(f)前記中継・監査サーバが、第2の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【0030】ここで、前記第1のサーバは、さらに、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、前記第2の要求メッセージの少なくとも一部の処理を委ねた第3の要求メッセージを第2のサーバに送信し、前記第2のサーバは、前記第2のメッセージを受信して、前記第1のサーバの公開鍵を用いて認証するとともに、これに回答した応答メッセージを自身の公開鍵暗号系の秘密鍵を用いた署名を付けて前記第1のサーバに送信し、前記第1のサーバは、受信した応答メッセージを前記第2のサーバの公開鍵を用いて認証した後に、第1の応答メッセージを前記中継・監査サーバに送信する、ようにしてもよい。

【0031】また、前記ステップ(c)における認証が異常であれば、前記第1のサーバは受信した第2の要求メッセージの処理を実行しないようにしてもよい。

【0032】また、前記ステップ(e)における認証が異常であれば、前記中継・監査サーバは第2の応答メッセージを前記クライアントに送信しないようにしてもよい。

【0033】また、さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含んでもよい。

【0034】また、本発明の第4の側面は、遠隔手続き呼び出しが実行可能なネットワーク・システムであって、サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、1以上の中継・監査サーバと、サービス要求メッセージを受信して、正当な経路を介して受信したメッセージであることを検査するとともに、要求されたメッセージに回答した応答メッセージを送信する、サービス・オブジェクトを有する1以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システムである。

【0035】また、本発明の第5の側面は、遠隔手続き呼び出しが実行可能なネットワーク・システムであつ

て、サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信し、その要求元を特定してから要求先のサーバに向けて転送するとともに、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、1以上の中継・監査サーバと、サービス要求メッセージを受信して、メッセージの送信元を特定するとともに、要求されたメッセージに回答した応答メッセージを送信する、サービス・オブジェクトを有する1以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システムである。

【0036】また、本発明の第6の側面は、遠隔手続き呼び出しが実行可能なネットワーク・システムであって、サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、サービス要求に対する応答メッセージを受信して、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、1以上の中継・監査サーバと、サービス要求メッセージを受信して、要求されたメッセージに回答した応答メッセージを送信する、サービス・オブジェクトを有する1以上のサーバとを具備し、前記中継・監査サーバ及びサーバは、メッセージ送信時には自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付け、メッセージ受信時には送信元の公開鍵を用いて認証を行うことを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システムである。

【0037】本発明の上記第4乃至第6の側面に係るネットワーク・システムにおいて、前記中継・監査サーバは、受信したサービス応答メッセージが正当なメッセージであることを検査してから要求元に向けて送信するとともに、要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するようにしてもよい。

【0038】また、本発明の第7の側面は、サービスを要求する1以上のクライアントと要求されたサービスを提供する1以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、サービス要求メッセージを受信する手段と、自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、を具備することを特徴とするサーバである。

【0039】また、本発明の第8の側面は、サービスを要求する1以上のクライアントと要求されたサービスを提供する1以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、サービ

ス要求メッセージを受信するとともにその要求元を特定する手段と、自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、を具備することを特徴とするサーバ。を特徴とするサーバである。

【0040】本発明の上記第7及び第8の側面に係るサーバにおいて、さらに、受信したサービス応答メッセージが正当なメッセージであることを検査する手段と、要求メッセージ及び／又は応答メッセージの送受信の履歴を記録する手段と、を含んでいてもよい。

【0041】また、本発明の第9の側面は、サービスを要求する1以上のクライアントと要求されたサービスを提供する1以上のサーバとで構成されるネットワーク上において実行される遠隔手続き呼び出し動作をサポートする中継・監視サーバであって、要求メッセージや応答メッセージの送受信を行う送受信部と、受信した要求メッセージを解析して要求パラメータを抽出する要求メッセージ解析部と、要求パラメータに所定の情報を連結して電子署名する監査証生成部と、応答メッセージを解析して、送信元のサーバが電子署名した受領証を抽出する応答メッセージ解析部と、受領証を電子認証する受領証処理部と、を含むことを特徴とする中継・監視サーバである。

【0042】

【作用】本発明に係る分散型のネットワーク・システムには、サービスを要求する1以上のクライアントと、サービス・オブジェクトを有する1以上のサーバが存在する。

【0043】サーバは、ある1つのサービス要求に対して、自身が所有するサービス・オブジェクトのみを以って応答してもよいが、他のサーバとの協働的動作によって応答しても良い。サーバ同士は、例えばCGI (Common Gateway Interface) のような接続形態によって協働的動作を実現することができる。

【0044】本発明においては、サービスを要求するクライアントは、サービス・オブジェクトを有するサーバに直接アクセスすることせず、中継・監査サーバに対してサービス要求メッセージを送信する。この中継・監査サーバは、ネットワーク・システム上のいずれかの場所に配設されているものとする。

【0045】ネットワーク・システムがインターネットであれば、サーバは例えば無数のHTML (Hyper Text Markup Language) ファイルを所有するHTTP (Hyper Text Transfer Protocol) サーバであり、サービス・オブジェクトはHTMLファイル (ホームページ) である。また、クライアントはURL (Unif o

rm Resource Locator) の送信という形態でサービス要求メッセージを送信することができる。

【0046】中継・監査サーバは、クライアントからの要求メッセージを受信すると、この受信メッセージに自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、該当するサービス・オブジェクトを持つサーバに向けて送信する。ここで、中継・監査サーバは、要求メッセージを中継する際に、サービスの要求元であるクライアント・ユーザを特定してもよい。特定することによって、中継・監査サーバは、要求メッセージの出所を証明したり、受信ログを記録することができる。また、中継・監査サーバはメッセージの送信ログを記録してもよい。

【0047】サービス・オブジェクトを持つサーバは、中継・監査サーバを介して要求メッセージを受け取ると、中継・監査サーバの公開鍵を用いて認証し、サービス要求の出所を確認することができる。認証を行うことによって、サーバは安心してサービスを提供することができる。

【0048】サーバは、自身が所有するサービス・オブジェクトのみを以って要求メッセージに応答する。この場合は、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、中継・監査サーバに応答メッセージを送信する。

【0049】あるいは、サーバは、要求されたサービスの処理の一部を他のサーバ (例えば木構造を形成する子サーバ) に委ねることができる。この場合、サーバは自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、要求メッセージを他のサーバに送信する。

【0050】サーバから要求メッセージを受け取った他のサーバ (子サーバ) は、公開鍵を用いて要求元のサーバを認証する。そして、応答メッセージを戻すときには、自身の公開鍵暗号系の秘密鍵を用いた署名を行う。他のサーバは、さらに他のサーバ (孫サーバ) にサービスを要求することもできるが、この場合は同様に、要求メッセージ送信時における署名と応答メッセージ受信時における認証を伴う。

【0051】サーバが要求サーバに回答した応答メッセージは、クライアントに戻される前に、一旦、中継・監査サーバにて受信される。この応答メッセージには、サーバの署名が付加されている。応答メッセージが複数のサーバの連携によって形成されているときには、これに関わった全て (又は少なくとも一部) のサーバの署名が応答メッセージに付加されている。中継・監査サーバは、各サーバの公開鍵を用いて署名を認証して、サービス・オブジェクトの出所を確認する。さらに、中継・監査サーバは、応答メッセージの中身がサービス要求に対する正当なメッセージであるかどうかを検査する。応答メッセージの内容が異常若しくは不当なものであれば、例えば再送要求を発行したり警告を発したりしてもよい。

【0052】このような認証や検査工程を経て、応答メッセージが中継・監視サーバから要求元クライアントに送信される。応答メッセージはその出所が明らかであり、内容も検査済みであるから、クライアントは信頼してこれを受理することができる。

【0053】また、中継・監視サーバは、要求メッセージや応答メッセージの送受信の履歴を記録し、遠隔手続き呼び出し動作を監視することができる。例えば、要求元のクライアントが同じサービス要求を頻繁に発行しているなど、ある特定のクライアント・ユーザがネットワーク上で不信な挙動を行っているときには、要求先のサーバ側に通知したりクライアントに警告を発したりしてもよい。

【0054】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0055】

【発明の実施の形態】以下、図面を参照しながら本発明の実施例を詳解する。

【0056】図1には、本発明の実施に供されるネットワーク・システム100の構成を模式的に示している。ネットワーク・システム100は、データ（すなわちサービス要求メッセージやサービス応答メッセージなど）の伝送媒体であるネットワーク10に無数のデータ端末装置50A、50B…が接続されており、分散コンピューティング環境を提供している。以下、各部について説明する。

【0057】ネットワーク10は、例えば大学や企業の構内などの限られた空間内に敷設されたLAN（Local Area Network）である。あるいは、LAN同士を専用線等で相互接続してなるWAN（Wide Area Network）や、一般公衆回線（PSTN: Public Switched Telephone Network）、ISDN（Integrated Service Digital Network）、これらネットワークの大規模な集合体であるインターネットであってもよい。各データ端末装置50A…は、モデムやTA（Terminal Adapter）、LANアダプタ等を介してネットワーク10に接続される。

【0058】データ端末装置50A…の一部はサービスを提供するサーバであり、その他はサービスを要求するクライアントである。データ端末装置50A…は、サーバ或いはクライアントとしてデザインされた専用のマシンであってもよいが、多くの場合は、サーバ用又はクライアント用のアプリケーションを導入して動作する汎用のコンピュータ・システムである。各データ端末装置同士は、ネットワーク10を介して、例えばTCP/IP（Transmission Control Protocol/Internet Protocol）接続

されている。

【0059】サーバは、複数のサービス・オブジェクトを所有しており、サービス要求に応じて適宜サービス・オブジェクトを要求元に提供する。サービス・オブジェクトの一例は、ホームページを形成するためのHTML（Hyper Text Markup Language）ファイルであり、HTTP（Hyper Text Transfer Protocol）プロトコルに従ってネットワーク10経由で伝送することができる。また、クライアントは、URLの形式に従って所望のサービス・オブジェクトを指定することができる。

【0060】ネットワーク10を介したURLによるサービス要求は、一種の遠隔手続き／メソッド呼び出しである。また、サーバは、ある1つのサービス要求に対して、自分一人で実行するとは限らず、さらに別のサーバにサービスの一部の提供を委ねることもある。サーバが他のサーバにサービスの提供を要求する方式の1つはCGI（Common Gateway Interface）である。すなわち、クライアントからのサービス要求を第1に受け取ったサーバ（仮に「親サーバ」とする）は、ホームページ内におけるコンテンツの一部の生成を別のサーバ（仮に「子サーバ」とする）に委ねる。そして、親サーバは、自ら生成したコンテンツと子サーバから戻されたコンテンツとからホームページを生成して、クライアントに戻すという仕組みである。さらに子サーバは自分の子サーバ（「孫サーバ」）にサービスの一部の提供を委ねることもある。サービスを提供する複数のサーバの親子関係は、一種の木構造を形成する。このような場合、要求されたサービスに対する応答は、木構造をなす各サーバ間の協働的な連携作業によって果たされる。

【0061】例えば、WWWクライアントがブラウザ画面上で検索項目を入力したときは、WWWサーバは、検索の実行と検索結果の送信を他のデータベース・サーバに要求することがある。この場合、データベース・サーバは、CGIなどの仕組みによってWWWサーバに連動して、要求されたサービスの一部を提供する。すなわち、データベース・サーバは、検索結果を示すテーブル中の該当カラムの内容を生成し、WWWサーバはテーブルの残りの部分を生成する（前述）。

【0062】本発明において特にユニークなのは、ネットワーク10上に存在するサーバの少なくとも1つが「中継・監視サーバ」として機能する点である。この中継・監視サーバは、クライアントに代行してサーバにサービス要求を行うようになっている。クライアントは、サーバに直接アクセスせず、中継・監視サーバに対してサービス要求メッセージを送信し、また、中継・監視サーバを経由してサービス応答メッセージを受信する。

【0063】中継・監視サーバは、メッセージ受信の際には送信元の認証を行うことでメッセージの内容を保証

する。メッセージ送信の際には、自ら署名を行うことで、メッセージの出所証明を行う。クライアントは、中継・監視サーバを介することで、安心してサービスの提供を受けることができる。また、中継・監視サーバは、サービスを要求するクライアント・ユーザを特定したり、そのログを記録することで、ユーザの不信な挙動をも監視する。中継・監視サーバを含んだメッセージ送受信オペレーションの詳細については後述に委ねる。

【0064】図2には、クライアントからのあるサービスを提供するために形成されたサーバの木構造を模式的に示している。同図では、サービスを提供する親サーバ3には2つの子サーバ4及び5が存在し、さらに子サーバ5を後継する孫サーバ6が存在する。但し、全てのサーバが同一の運営団体に所属しているとは限らない。また、クライアント1とサーバ4の間には、中継・監視サーバ2が介在している。中継・監視サーバ2は、その機能実現のために特化してデザインされたデータ端末装置であってもよいが、中継・監視サーバ用のアプリケーション・プログラムを導入した汎用コンピュータ・システムであってもよい。

【0065】図3には、本発明を実現する中継・監視サーバ2の構成を模式的に図解したブロック図である。同図に示すように、中継・監視サーバ2は、監査証作成部210と、要求メッセージ解析部220と、送受信部230と、受領証処理部240と、応答メッセージ解析部250とで構成される。以下、各部について説明する。

【0066】送受信部230は、ネットワーク10経由でのメッセージの送受信を行うための装置である。クライアント1に対しては、サービス要求メッセージの受信とサービス応答メッセージの送信を行う。また、サーバ3に対しては、サービス要求メッセージの送信と、サービス応答メッセージの受信を行う。

【0067】要求メッセージ解析部220は、送受信部230から受け取ったサービス要求メッセージの解析処理を行う。また、要求メッセージ中の要求パラメータを抽出して監査証作成部210に渡す。

【0068】監査証生成部210は、電子署名を行うために、公開鍵暗号系の秘密鍵を所有する。要求メッセージ解析部220から要求パラメータを渡されると、これに監査証番号とその有効期限を表した文字列を連結して、さらに秘密鍵を用いて電子署名する。この電子署名は、中継・監視サーバ2が発行する監査証を意味する。この後、監査証が付された要求メッセージは、送受信部230から送出される。また、監査証生成部210は、クライアントからの要求メッセージを管理するためのログ・ファイルを備えており、クライアントからの要求メッセージを処理する度に、ログをとるようになってい

る。

【0069】応答メッセージ解析部250は、サーバから受信した応答メッセージの解析処理を行う。応答メッ

セージには、送信元のサーバによって電子署名が施された受領証が含まれている。応答メッセージ解析部250は、応答メッセージから受領証を抽出して、受領証処理部240に渡す。

【0070】受領証処理部240は、各サーバ3、4、5、6の公開鍵を保持しており、応答メッセージ解析部250から渡された受領証の署名の認証を行う。本実施例では、サーバ3から戻されたサービス応答メッセージ中には、サービス応答に携わった全て（又は少なくとも一部）のサーバ3、4、…の電子署名が施されている

（後述）。これら電子署名は、各サーバ3、4、…の受領証の役割を持つ。受領証処理部240は、該当するサーバの公開鍵を用いて各署名を電子認証する。また、受領証処理部240は、各サーバ毎のログ・ファイルを管理しており、認証手続きに成功したときには該当するサーバのログ・ファイルにそのログを追加するようになっている。

【0071】なお、図3に示した各ブロックは、専用のハードウェア装置としてデザインすることも、或いは汎用コンピュータ・システムに導入されたプログラム・モジュールの形態で実装することも可能である。

【0072】図4には、本発明の実施に供されるサーバ3の構成を模式的に図解したブロック図である。同図に示すように、サーバ3は、サービス・オブジェクト部310と、応答メッセージ生成部320と、要求メッセージ解析部330と、送受信部340と、応答メッセージ解析部350と、要求メッセージ生成部360とで構成される。以下、各部について説明する。

【0073】送受信部340は、ネットワーク10経由でのメッセージの送受信を行うための装置である。中継・監視サーバ2若しくは自分の親サーバに対しては、サービス要求メッセージの受信とサービス応答メッセージの送信を行う。また、自分の子サーバに対しては、サービス要求メッセージの送信と、サービス応答メッセージの受信を行う。

【0074】サービス・オブジェクト部310は、サーバ3がサービス要求に回答して提供するサービス・オブジェクトの集合で構成される。サービス・オブジェクトの一例は、WWWクライアントのディスプレイ上においてホームページを形成するためのHTMLファイルである。サービス・オブジェクト部310の実体は、サービス・オブジェクトを格納するディスク型格納装置である。クライアント1や子サーバに対してサービスを要求する親サーバは、所望のサービス・オブジェクトをURLによって指定することができる。

【0075】要求メッセージ解析部330は、送受信部340から受け取ったサービス要求メッセージを解析処理する。ここで言う解析処理は、要求メッセージ中の監査証を抽出して、該メッセージの有効性や正当性などのチェックを行うことである。要求メッセージ解析部33

0は、既に無効となった監査証の識別子を管理するための無効識別子テーブルも備えている。

【0076】要求メッセージ解析部330は、要求メッセージ送信元の公開鍵を用いて監査証を電子認証するとともに、監査証中の有効期限を検証する。有効期限が消滅していれば、次のステップには進まないで、サービス・オブジェクトの提供は行われない。監査証が有効期限内であれば、次に、監査証の識別子が無効識別子テーブル中にないかどうかを確認する。テーブル中に存在すれば、監査証が既に無効であることを意味するので、次のステップには進まず、この結果としてサービス・オブジェクトの提供は行われない。監査証の識別子が無効識別子テーブル中になければ、該識別子を該テーブル中に追加する。この結果、同一の監査証の流用が禁止されることになる。

【0077】監査証の検査を終えた後、要求メッセージ解析部330は、要求メッセージ中の要求パラメータをサービス・オブジェクト部310に渡す。サービス・オブジェクト部310は、これに応答して、該当するサービス・オブジェクトを自ら所有するときには、該サービス・オブジェクトを応答メッセージ生成部320に供給する。また、該当するサービス・オブジェクトを自らは所有せず、サーバ3の子孫のサーバ4、5…が所有するときには、要求メッセージ生成部360に対して子孫サーバ4、5…へのサービス要求メッセージの送信を促す。

【0078】応答メッセージ生成部320は、サービス・オブジェクト部310から取り出されたサービス・オブジェクトを基にして、応答メッセージを生成する。また、応答メッセージ生成部320は、公開鍵暗号系の秘密鍵を所有しており、応答メッセージに対して電子署名を行うことによって、応答メッセージに受領証を添付する。受領証着きの応答メッセージは送受信部340によってサービス要求元に送出される。

【0079】要求メッセージ生成部360は、子孫サーバ4、5…に対して送信するサービス要求メッセージを生成するためのものである。要求メッセージ生成部360は、公開鍵暗号系の秘密鍵を所有しており、要求メッセージに対して電子署名を行うことにより要求メッセージに監査証を添付する。監査証付きの要求メッセージは、送受信部340によってサービス要求先に送出される。なお、子孫サーバ4、5…へのサービス要求は、例えばCGI(Common Gateway Interface)の形態で行われる。

【0080】応答メッセージ解析部350は、送受信部340が受信した子孫サーバ4、5…からの応答メッセージを解析するためのものである。応答メッセージには、サービス要求に応答した全て(又は少なくとも一部)の子孫サーバ4、5…の電子署名を含んだ受領証が添付されている。応答メッセージ解析部350は、各子

孫サーバ4、5…の公開鍵を用いて受領証を電子認証する。また、子孫サーバ4、5…から送られてきたサービス・オブジェクトに加えて、サーバ3自身が所有するサービス・オブジェクトを送るときには、サービス・オブジェクト部310に対して所望のサービス・オブジェクトの取り出しを促す(例えば、サーバ3がホームページ上のテーブルを作成し、該テーブル中の所定のカラムを子孫サーバ(データベース・サーバなど)が作成する場合がこれに該当する)。

10 【0081】以下でも詳解するが、サーバ3は、サービス・オブジェクトを提供するサーバそのものとして機能する以外に、自分の子孫にあたる各サーバ4、5、6からの応答メッセージを認証する認証局としての役割も持つ、という点を充分理解されたい。

【0082】なお、図4に示した各ブロックは、専用のハードウェア装置としてデザインすることも、或いは汎用コンピュータ・システムに導入されたプログラム・モジュールの形態で実装することも可能である。

【0083】また、サーバ3の子孫にあたるその他のサーバ4、5、6も、図4に示したものと同様の構成を具備するものと理解されたい。例えば、図示しないサーバ4は、サービス・オブジェクト部410と、応答メッセージ生成部420と、要求メッセージ解析部430と、送受信部440と、応答メッセージ解析部450と、要求メッセージ生成部460とで構成される。

【0084】次いで、ネットワーク・システム100上における遠隔手続き呼び出しの処理動作について説明する。図5には、クライアント1が発行したサービス要求が中継・監視サーバ2及び各サーバ3、4、5…の協働的動作によって処理される様子を模式的に示している。

【0085】この例では、各サーバ3、4、5…はHTTPサーバであり、クライアント1はHTTPプロトコルを用いてサービス要求メッセージを送信するものとする。また、サーバ3は、自分の子孫サーバ4、5…と連携して、HTMLで記述された1つのファイルを生成するものとする。例えば、サーバ3がHTMLファイルに含まれるテーブルの前半部分に該当するサービス・オブジェクトを提供し、その子孫サーバ4がテーブルの後半部分に該当するサービス・オブジェクトを提供する。サーバ3、4、5…同士は、例えばCGI(Common Gateway Interface)に従った手順によって接続される。ここでは、各々のサーバ3、4、5…のドメイン名を仮に"server300"、"server400"、"server500"…としておく。

【0086】クライアントは、HTTPプロトコルを用いて、以下のような第1のサービス要求メッセージ(service1)を中継・監視サーバに送信する。

【0087】

50 【数1】GET /service1 HTTP/1.

1

【0088】中継・監視サーバ2は、第1のサービス要求メッセージを受信すると、これを要求メッセージ解析部220に渡す。

【0089】要求メッセージ解析部220は、第1のサービス要求メッセージ中の要求パラメータとして"service1"を抽出する。次いで、自身が持つURL対応テーブルを検索して、"service1"に対応するURL"http://server300/object310"を取り出して、これを監査証生成部210に渡す。このURLは、ドメイン名"server300"を持つサーバ3のサービス・オブジェクト部が所有するサービス・オブジェクト"object310"を要求するものとする。

【0090】監査証生成部210は、メッセージの識別子、有効期限、サービス名の3項のパラメータからなる以下のようなデータを生成する。

【0091】

【数2】

(1, 199806081010:199806081015, service1)

【0092】上記の3項組のデータは、識別子が1、有効期限(但し世界時刻とする)が1998年6月8日10時10分から同日の10時15分まで、サービス名がservice1であること、すなわち、識別子1を持つサービス要求に対しては1998年6月8日10時10分から同日10時15分までの間service1へのアクセスが許可されていることを示している。この3項組のデータは、要するにサービス・オブジェクトに対するアクセス権限を意味する。ネットワーク・コンピューティング関連の技術分野ではアクセス権限は「ケーパビリティ(Capability)」とも呼ばれる。

【0093】監査証生成部210は、この3項組のデータに対してメッセージ・ダイジェスト関数を適用し、自身が保持する公開鍵暗号系の秘密鍵secretkey1を用いて電子署名を行う。ここで付された署名は、後続のサーバ3において「監査証10」の役割を果たすが、以下では"signature1"と呼ぶことにする。

【0094】監査証生成部210は、要求された"service1"に対応するURL"http://server300/object310"を基にして、サーバ3の送受信部340に対して以下のような第2のサービス要求メッセージを送信する。

【0095】

【数3】

GET /object310 HTTP/1.1

Capability: (1, 199806081010:199806081015, service1)

Signature: signature1

【0096】サーバ3の送受信部340は、第2のサー

ビス要求メッセージを受け取ると、これを要求メッセージ解析部330に渡す。要求メッセージ解析部330は、これに回答して以下の工程を実行する。

【0097】(1) メッセージの先頭行からサービス・オブジェクトの名前を抽出して、該サービス・オブジェクトについての第1のリファレンスを得る。

(2) HTTPにおけるリクエスト・ヘッダのうち"Capability"というフィールド名に対応する値を抽出して、第1のケーパビリティとする。

(3) HTTPにおけるリクエスト・ヘッダのうち"Signature"というフィールド名に対応する値を抽出して、第1の署名とする。

(4) 第1のケーパビリティに記述された有効期限が期限内かどうかを検査する。期限内であれば次工程に進むが、そうでなければ当該ケーパビリティが無効である旨の応答メッセージを送受信部340に入力する。

(5) 第1のケーパビリティが無効識別子テーブルの中に存在するかどうかを検索する。該テーブル中になければ次工程に進むが、そうでなければ当該ケーパビリティが無効である旨の応答メッセージを送受信部340に入力する。

(6) 中継・監視サーバ2の公開鍵を用いて、第1の署名が第1のケーパビリティの正しい署名であるかどうかを検査する。正しい署名であれば、第1のケーパビリティの識別子を無効識別子テーブルに追加する。

(7) 第1のリファレンスで示されるサービス・オブジェクト部310に要求メッセージを渡す。また、第1のケーパビリティと第1の署名を要求メッセージ生成部360に入力する。

【0098】一度受理したケーパビリティの識別子を無効識別子テーブルに登録しておくことにより、ネットワーク上の不正者が同じケーパビリティを流用するのを防止することができる。

【0099】第2のサービス要求メッセージに回答するために、さらにサーバ4が持つサービス・オブジェクトを必要とするときには、サーバ3のサービス・オブジェクト部310は、サーバ4のサービス・オブジェクト部410にサービス要求メッセージを送信すべく、要求メッセージ生成部360に要求メッセージの生成を要求する。

【0100】要求メッセージ生成部360は、サーバ3自身が所持する公開鍵暗号系のsecretkey2を用いて第2の署名signature2を作成し、第1のケーパビリティと第1の署名と第2の署名(すなわち「監査証20」)を含んだ第3のサービス要求メッセージを生成する。

【0101】サーバ3は、サーバ4に対して、HTMLファイル中のテーブルの後半部分を要求するものとする。この場合、第3のサービス要求メッセージは以下のようになる。

【0102】

【数4】

GET /object410 HTTP/1.1

Capability: (1, 199806081010:199806081015, service1)

Signature: signature1

Signature: signature2

【0103】サーバ4の要求メッセージ解析部430は、第3のサービス要求メッセージを受け取ると、以下の工程を実行する。

【0104】(1) メッセージの先頭行からサービス・オブジェクトの名前を抽出して、サービス・オブジェクトの第2のリファレンスを得る。

(2) HTTPにおけるリクエスト・ヘッダの形式のうち「Capability」というフィールド名に対応する値を抽出して、第1のケーパビリティ（アクセス権限）とする。

(3) HTTPにおけるリクエスト・ヘッダの形式のうち「Signature」というフィールド名に対応する値を抽出して、第1の署名とする。

(4) HTTPにおけるリクエスト・ヘッダの形式のうち「Signature2」というフィールド名に対応する値を抽出して、第2の署名とする。

(5) 第1のケーパビリティの有効期限が期限内であるかどうかを検査する。期限内であれば次工程に進むが、そうでなければ該ケーパビリティが無効である旨の応答メッセージを送受信部410に渡す。

(6) 第1のケーパビリティの識別子が無効識別子テーブルの中にあるかどうかを検索する。該テーブル中になければ次工程に進むが、そうでなければ該ケーパビリティが無効である旨の応答メッセージを送受信部410に入力する。

(7) 第1の署名が第1のケーパビリティの正しい署名であるかどうかを、中継・監視サーバ2の公開鍵を用いて検査する。正しい署名であれば、第1のケーパビリティの識別子を無効識別子テーブルに追加する。

(8) 第2の署名が第1のケーパビリティの正しい署名であるかどうかを、サーバ3の公開鍵を用いて検査する。正しい署名であれば次工程に進むが、そうでなければ工程を中止する。

(9) 第1のリファレンスで示されるサービス・オブジェクト部410に要求メッセージを渡す。また、第1のケーパビリティと第1の署名を要求メッセージ生成部460に入力する。

【0105】一度受理したケーパビリティの識別子を無効識別子テーブルに登録しておくことにより、ネットワーク上の不正者が同じケーパビリティを流用するのを防止することができる。

【0106】要求メッセージを受け取ったサービス・オブジェクト部410は、要求されたHTMLファイル中

のテーブルの後半部分を生成する。サービス・オブジェクト部410が提供するサービス・オブジェクトの実体は、例えば以下のようなものである。

【0107】

【数5】

<tr>

<td> b b b b 1 0 0

<td> 1 0 0

<td> 1 0 0 0

10 <tr>

<td> b b b b 2 0 0

<td> 2 0 0

<td> 2 0 0 0

<tr>

<td> b b b b 3 0 0

<td> 3 0 0

<td> 3 0 0 0

【0108】サービス・オブジェクト部410は、このような「文書1」を生成して、応答メッセージ生成部420に渡す。

20

【0109】応答メッセージ生成部420は、サーバ4が所持する公開鍵暗号系の秘密鍵を用いて文書1に署名を施すことでサービス応答メッセージを生成する。そして、送受信部440を介してサーバ3の送受信部340にサービス応答メッセージを送信する。サービス応答メッセージに付された署名は「受領証30」としての意味を持つ。

【0110】サーバ3の送受信部340は、サービス応答メッセージを受け取ると、これを応答メッセージ解析部350に渡す。

30

【0111】応答メッセージ解析部350は、サービス応答メッセージを解析し、サーバ4の公開鍵を用いて署名の認証を行う。この認証作業は、サーバ3が自分の子孫にあたる各サーバ4、5、6に対する認証局としての役割も持つことを意味する。

【0112】署名が正しく認証されたならば、応答メッセージ解析部350はサービス応答メッセージ中の文書1をサービス・オブジェクト部310に渡す。

【0113】サービス・オブジェクト部310は、要求されたHTMLファイル中のテーブルの前半部分を生成する。サービス・オブジェクト部410が提供するサービス・オブジェクトの実体は、例えば以下に示すような「文書2」である。

【0114】

【数6】

<tr>

<td> a a a a 1 0 0

<td> 1 0 0

<td> 1 0 0 0

50 <tr>

```

<td> aaaa200
<td> 200
<td> 2000
<tr>
<td> aaaa300
<td> 300
<td> 3000

```

【0115】サービス・オブジェクト部310は、上述の文書1と文書2とを連結して「文以下に示すような「文書3」を生成する。

【0116】

【数7】

```

<html>
<head>
<title>表の合成結果</title>
</head>
<body>
<table>
<tr>
<td> aaaa100
<td> 100
<td> 1000
<tr>
<td> aaaa200
<td> 200
<td> 2000
<tr>
<td> aaaa300
<td> 300
<td> 3000
<tr>
<td> bbbb100
<td> 100
<td> 1000
<tr>
<td> bbbb200
<td> 200
<td> 2000
<tr>
<td> bbbb300
<td> 300
<td> 3000
</table>
</body>
</html>

```

【0117】生成された文書3は、応答メッセージ生成部320に渡される。

【0118】応答メッセージ生成部320は、サーバ3が所持する公開鍵暗号系の秘密鍵を用いて文書3に署名を行い、サービス応答メッセージを生成する。サービス

応答メッセージに付された署名は、「受領証80」としての意味を持つ。そして、サービス応答メッセージは、送受信部340を介して中継・監査サーバ2の送受信部240に送信される。

【0119】中継・監視サーバ2の送受信部240は、受け取ったサービス応答メッセージを応答メッセージ解析部250に渡す。

【0120】応答メッセージ解析部250は、サーバ3及びサーバ4の各々の公開鍵を用いて監査証80に含まれる各署名を検査する。すなわち、中継・監視サーバ2は、サービスを提供する各サーバ3、4…に対する認証局として機能する。

【0121】正しく認証されたときには、文書3は送受信部240を介してクライアント1に送信されるが、認証に失敗したときには、文書3に代わって、サービス応答メッセージが正しくない旨の応答メッセージを送信する。

【0122】なお、上記の説明では、クライアント1からのサービス要求に対して、サーバ3はサーバ4とのみ連携して応答する例を挙げたが、サーバ3がサーバ5及びサーバ6と連携する場合も同様である。このような場合、サーバ3がサーバ5に要求メッセージを送信するときには「監査証40」が、サーバ5がサーバ6に要求メッセージを送信するときには「監査証50」が、夫々添付される。また、サーバ6がサーバ5に応答メッセージを送信するときには「受領証60」が、サーバ5がサーバ3に応答メッセージを送信するときには「受領証70」が、夫々添付される。

【0123】また、上述の実施例では、ネットワークを介してコンピュータ同士がメッセージを送受するためのプロトコルとしてHTTPを取り上げたが、他の任意のプロトコルを使用しても同様に本発明を適用することができる。プロトコルは、例えば、HTTPS、S-HTTP (secure HTTP)、FTP (File Transfer Protocol)、CORBA (Common ORB Architecture)、IIOP (Internet Inter-ORB Protocol)、JavaRMI (Remote Method Invocation) のいずれであってもよい。

【0124】〔追補〕以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0125】

【発明の効果】以上詳記したように、本発明によれば、

1以上のサーバと1以上のクライアントからなる分散型のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための、優れた遠隔手続き呼び出しを行う方式を提供することができる。

【0126】また、本発明によれば、少なくとも1つの中継・監査サーバを中継してサービスの要求がサーバに届くようなタイプの、優れた遠隔手続き呼び出し方式を提供することができる。

【0127】また、本発明によれば、複数のサーバの協働的な動作によってクライアントから要求されたサービスを提供するような分散型のネットワーク環境において、サービスの正当な履行を保証するための優れた方式を提供することができる。

【0128】また、本発明によれば、ネットワーク上に中継・監査サーバを配設することで、サービス要求の出所を認証したり、サーバから提供されたサービスを保証することができる、優れた遠隔手続き／メソッド呼び出し方式を提供することができる。

【図面の簡単な説明】

【図1】 本発明の実施に供されるネットワーク・システム100の構成を模式的に示した図である。

【図2】 クライアントからのあるサービスを提供するために形成されたサーバの木構造を模式的に示した図である。

【図3】 本発明を実現する中継・監視サーバ2の構成を模式的に示したブロック図である。

【図4】 本発明の実施に供されるサーバ3の構成を模式的に示したブロック図である。

【図5】 ネットワーク・システム100上において遠隔手続き呼び出しを処理するためのオペレーションを模式的に示した図である。

【図6】 ネットワーク上で、WWWサーバがデータベース・サーバと協調してクライアントから呼び出された遠隔手続きを処理する様子を模式的に示した図である。

【図7】 ネットワーク上において、多数のサーバが連携してクライアントのサービス要求に応答する様子を模式的に示した図であり、より具体的には、多数のサーバはサービス要求／応答に関する木構造を形成し、且つ、各サーバは互いに異なる組織に属している様子を模式的に示した図である。

【図8】 ネットワーク上において、多数のサーバが連携してクライアントのサービス要求に応答する様子を模式的に示した図であり、より具体的には、一部の子サーバがダミーのクライアントを用いて不正なサービス要求を発行する様子を模式的に示した図である。

【符号の説明】

100…ネットワーク・システム

210…監査証生成部

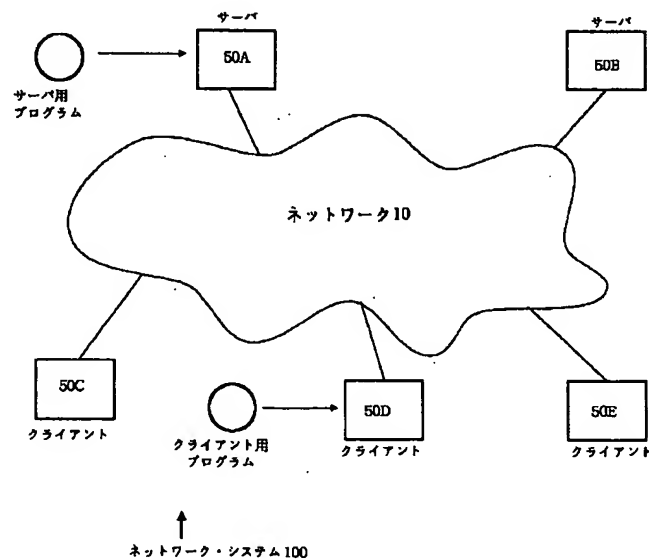
220…要求メッセージ解析部

230…送受信部

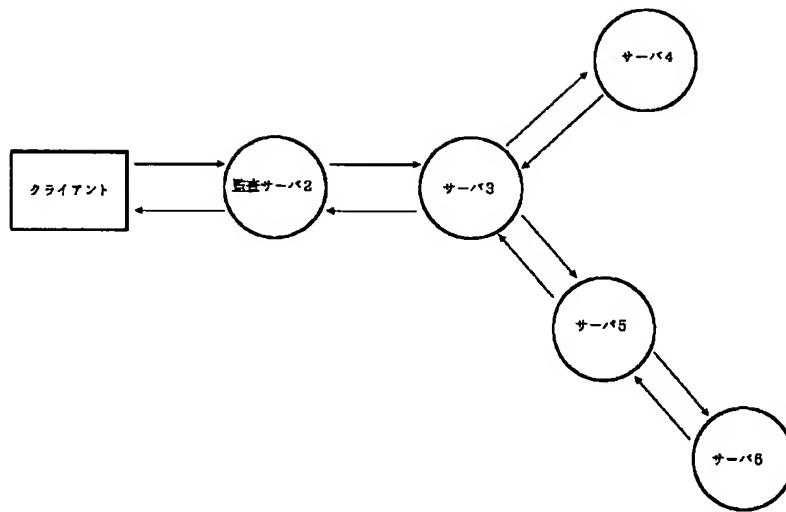
240…応答メッセージ解析部

250…受領証生成部

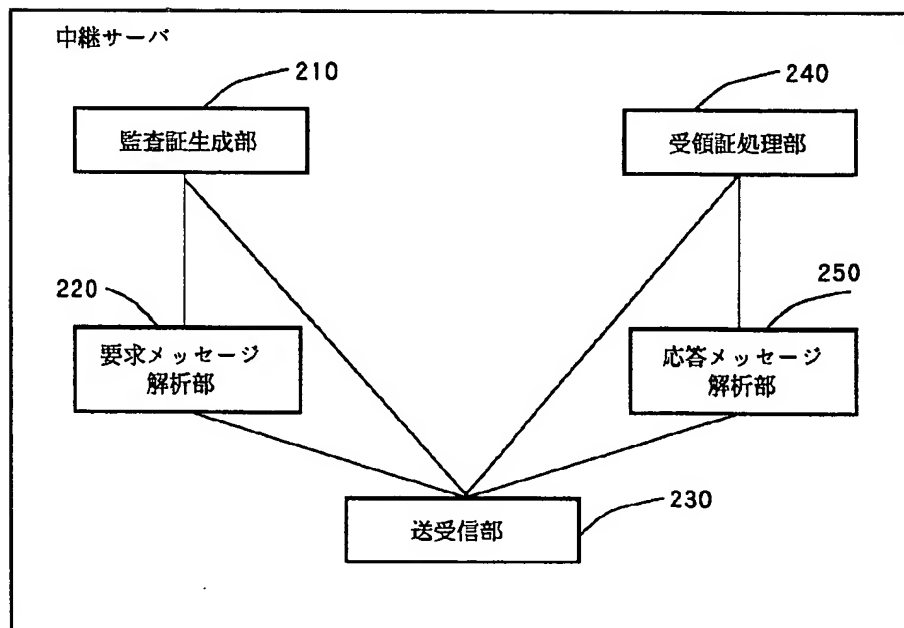
【図1】



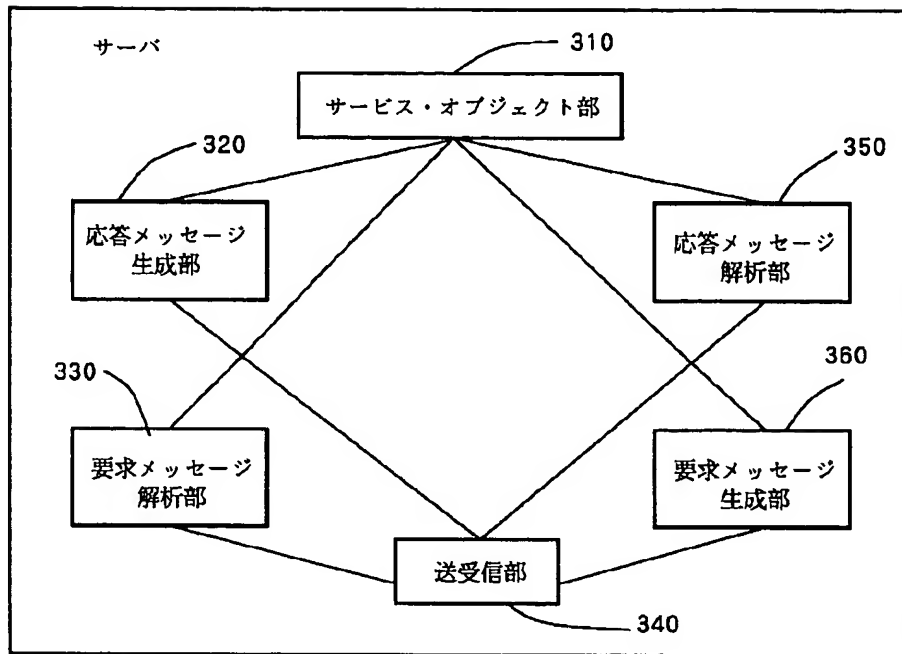
【図 2】



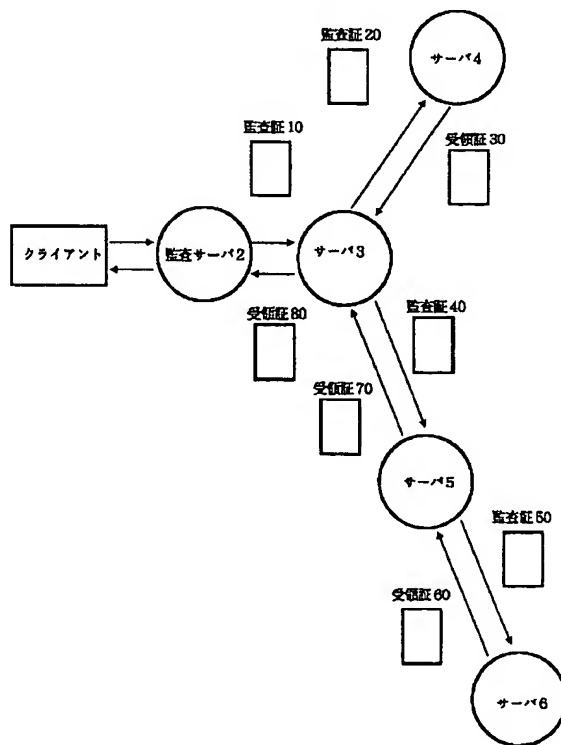
【図 3】



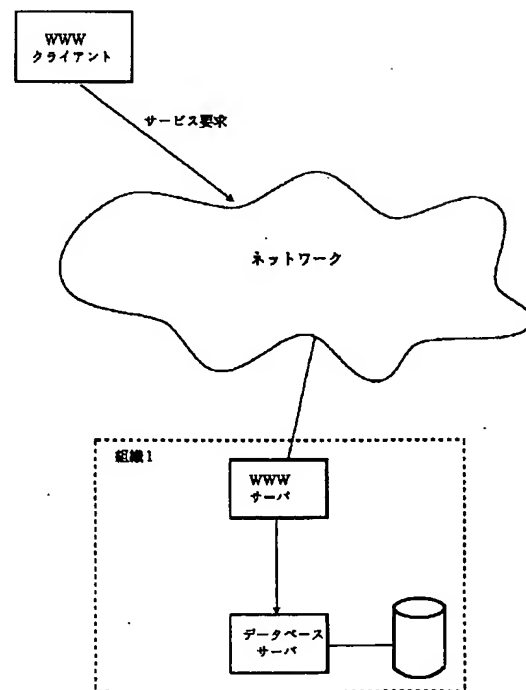
【図 4】



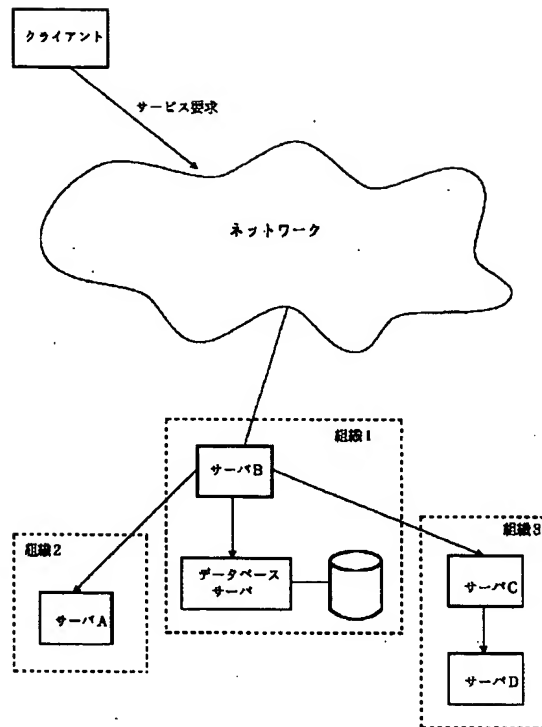
【図 5】



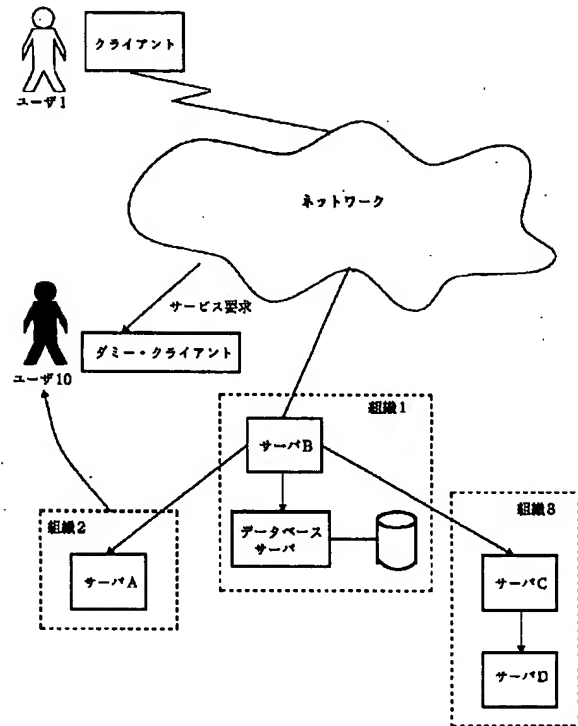
【図 6】



【図7】



【図8】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☐ FADED TEXT OR DRAWING

☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.